Overview of Massachusetts Data Security Laws

Scott D. Schafer
Assistant Attorney General
Consumer Protection Division
Office of Massachusetts
Attorney General Martha Coakley

Massachusetts Identity Theft Legislation

August 3, 2007

Massachusetts adopts comprehensive identity theft legislation

Becomes the 39th state to protect residents by requiring that they be notified in the event of a data security breach or unauthorized access or use of their personal information.

Massachusetts Identity Theft Legislation

Major Provisions of the Legislation

1) Establishes a consumer's right to request a security freeze (G.L. ch. 93, §§56 and 62A);

2) Establishes requirements for notification to state government and consumers in the event of a data breach (G.L. ch. 93H); and

3) Establishes requirements for destruction and disposal of records containing a consumer's personal information (G.L. ch. 93I).

Security Breaches
G.L. ch. 93H

Who does the law apply to?

Any individual, business or governmental agency that owns, licenses, maintains or stores data whose unauthorized access or use is capable of compromising a Massachusetts resident's personal information.

Security Breaches
G.L. ch. 93H

What is personal information?

First name and last name or first initial and last name of a resident in combination with one or more of the following:

1. **SSN;**
2. **driver's license number or state-issued card id number; or**
3. **financial account, debit or credit card number.**

Security Breaches
G.L. ch. 93H

Massachusetts law protects personal information regardless of form – paper or electronic.

Protected personal information does <u>not</u> include information that is lawfully obtained from publicly available information.

Security Breaches
G.L. ch. 93H

When is notice triggered?

1. **Breach of security**

2. **Personal information acquired or used by an unauthorized person; or**

3. **Personal information used for an unauthorized purpose.**

Security Breaches G.L. ch. 93H

Definition of "Breach of Security"

Unauthorized acquisition or use of unencrypted data or, encrypted electronic data and the confidential process of key that is capable of compromising the security, confidentiality of personal information, maintained by a person or agency that creates a substantial risk or identity theft or fraud against a Massachusetts resident.

Security Breaches G.L. ch. 93H

Definition of "Breach of Security"

Broader definition -- Breach need not involve "personal information" as defined in statute

Notice triggered if there is a substantial risk of ID Theft or fraud

Security Breaches G.L. ch. 93H

Personal Information Notification Triggers

Personal information acquired or used by unauthorized person

Personal information used for unauthorized purpose

Security Breaches G.L. ch. 93H

Personal Information Notification Triggers

No "substantial risk of harm" calculus.

Notification is triggered by the breach itself rather than the likelihood of harm or misuse of personal information.

Entities are therefore not exempt from providing notice if a breach does not create a risk of harm.

Security Breaches G.L. ch. 93H

Who must be notified?

1. **The Attorney General;**
2. **Director of Consumer Affairs and Business Regulation;**
3. **Information Technology Division;**
4. **Division of Public Records; and**
5. **Affected Residents**

Security Breaches G.L. ch. 93H

What must the notice say?

Massachusetts law has different content requirements depending on the recipient of the notice.

Security Breaches G.L. ch. 93H

Notice to the Attorney General and Director of Consumer Affairs and Business Regulation

1. **Nature of the breach of security or the unauthorized access or use of personal information;**

2. **Number of Massachusetts residents affected; and**

3. **Steps the notifying entity is taking, or plans to take, relating to the incident.**

Security Breaches G.L. ch. 93H

Notice to the Information Technology Division and Division of Public Records

Follow policies and procedures adopted by that division pertaining to reporting and investigation of incident

See e.g. ITD Cybercrime Security Incident Policy available at ITD's website under "Policies, Standards and Guidance" and "Security"

Security Breaches G.L. ch. 93H

Notice to Affected MA Residents

1. **Consumer's right to obtain police report;**

2. **How a consumer requests a security freeze;**
   G.L. 93, §§ 56 and 62A

3. **Information consumer will need to provide to request security freeze; and**

4. **Disclosure of fees associated with placing, lifting or removing a security freeze**

Security Breaches G.L. ch. 93H

Notice to Affected MA Residents

Notice to the affected residents shall not include:

1. **Nature of the breach or unauthorized access or use; or**

2. **The number of residents affected.**

Security Breaches G.L. ch. 93H

Common Mistakes Made in
Notices to Affected MA Residents

1. **Notice is too general and fails to include the four (4) Massachusetts specific requirements**

2. **Fraud Alert vs. Security Freeze**

Security Breaches G.L. ch. 93H

Common Mistakes Made in
<u>Notices to Affected MA Residents</u>

3. **References to websites rather than providing information in letter itself – thereby putting burden on affected residents to find information**

4. **Provides a range of fees relating to security freeze when in fact amount is set by statute (G.L. ch. 93, §62A)**

Security Breaches G.L. ch. 93H

Notice to Affected MA Residents

Law provides for direct notice to affected consumers unless:

1. **More than 500,000 affected MA residents; or**

2. **Costs of providing written notice shall exceed $250,000.**

"Substitute" notice consists of: 1) email notice to affected consumers; 2) clear and conspicuous notice on the company's home page; and 3) publication in statewide media.

Security Breaches G.L. ch. 93H

When must notice be provided?

"As soon as practicable and without unreasonable delay"

Massachusetts permits a delay where law enforcement determines notification would hinder a criminal investigation -- provided that the law enforcement agency notifies the Attorney General of that determination.

Most Common Causes of Data Breaches

1. Stolen Laptops
2. Rogue Employees
3. Inadvertent Disclosure
4. Intra-company Email
5. Hacking

Data Disposal G.L. ch. 93I

Scope of the Law

Requires individuals, businesses and governmental agencies to employ certain safeguards when disposing of or destroying records containing personal information – regardless of form.

Data Disposal G.L. ch. 93I

Minimum standard for disposal/destruction of records

Destruction of records containing personal information must be done in such a manner so that personal information "cannot practically be read or reconstructed."

Paper records shall be burned, redacted, pulverized or shredded so that personal information cannot be read or reconstructed.

Electronic records and other non-paper media shall be destroyed or erased so that personal information cannot be read or reconstructed.

Data Disposal G.L. ch. 93I

Third-party Disposal

May use third parties provided that the third parties adopt and monitor compliance with policies and procedures that prohibit unauthorized access to or use of personal information in the course of the collection, transportation or disposal of the information.

Entities employing such third-party services should obtain written assurances from the third party that its disposal practices are in compliance with the law.